ARIZONA CODE OF JUDICIAL ADMINISTRATION
Part 1: Judicial Branch Administration
Chapter 5: Automation
Section 1-506: Filing and Management of Electronic Court Documents

A. Definitions. In this section the following definitions apply:

"ANSI/AIIM" means the American National Standards Institute and the Association for Information and Image Management. These two organizations are responsible for promoting and facilitating voluntary consensus standards and conformity assessment systems and promoting their integrity.

"Browser" means a computer application that interprets hypertext markup language (HTML), the programming language of the Internet, into the words and graphics that are viewed on a web page.

"Checksum or hashing algorithm" means a formula or procedure for checking that electronically transmitted messages have not been altered. A checksum is a numerical value based on the number of bits in the message. A hashing function transforms a string of characters into a usually shorter fixed-length value or key that represents the original string. The results are sent with the message. The receiver of the message executes the same formula and compares the results to the value sent. Any difference indicates an alteration of the message.

"Cryptography" is the science of rendering plain information unintelligible and restoring encrypted information to intelligible form. As a way of achieving data security, encryption translates plain text into secret code that can only be decrypted by those with the secret key or password.

"Digital certificate" means an attachment to an electronic message used for security purposes. The most common use is as part of a digital signature process to verify the identity of the sender of a message.

"Digital time-stamp" means a cryptographically enabled time stamp which is digitally signed by a time stamp server and thus cannot be modified without detection. It provides information showing that a document existed before a given time.

"Electronic or digital signature" means digital code attached to an electronic message. An "electronic signature" means any letters, characters, or symbols executed with an intent to authenticate a writing. A "digital signature" is an electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a document, and possibly to ensure that the original content of the message or document that has been sent is unchanged.

"Electronic Document Management System (EDMS)" means a collection of computer software application programs and hardware devices that provides a means of organizing and controlling the

creation, management and retrieval of documents through their life cycle. It may include workflow software which enables organizations to define routing and processing schemes to automate the business processes for document handling. It may also include imaging and optical character recognition (OCR) software and devices to support the capture, storage, and retrieval of document images from paper.

"Electronic filing system@ means a collection of software application programs used to transmit documents and other court information to the court through an electronic medium, rather than on paper. An electronic filing system may include functions to send and receive documents, pay filing fees, and receive court notices and information.

AFile transfer protocol (FTP)@ means a standard Internet application protocol used to exchange files between computers on the Internet. It is commonly used to download programs and other files to a computer from other servers.

ANon-proprietary@ means material (particularly software) that is not subject to ownership and control by a third party. AProprietary@ generally refers to vendor-owned material whose specifications are not public.

APublic Key Infrastructure (PKI)@ is a system using digital certificates with an encryption methodology that has two keys, a public key and a private key. The keys are related in such a way that only the public key can be used to encrypt messages and only the corresponding private key can be used to decrypt them.

B. Purpose. This section provides administrative requirements, standards and guidelines to enable Arizona courts to achieve these goals:

1. To allow the electronic exchange of documents within the court system;

2. To assure that courts carefully plan the migration to an EDMS and select a system that is secure, flexible, robust and user-friendly;

3. To assure that courts establish an EDMS to manage, receive, docket, distribute, retrieve and access all internally generated and electronically filed documents; and

4. To assure that all Arizona courts implement electronic filing systems uniformly.

C. Authority. Only the chief justice, the chief judge of each division of the court of appeals, and the presiding judge of the superior court in each county may implement, consistent with these requirements and Rule 124, Rules of the Supreme Court of Arizona, an electronic filing system in their respective courts.

The presiding judge of the superior court in each county may implement, consistent with these requirements and Rule 124, an electronic filing system in one or more justice courts or municipal courts within the county.

D. Document Specifications. Documents filed or delivered electronically shall comply with the following:

1. All documents shall be preserved so that the content of the original document is not altered in any way and the appearance of the document when displayed or printed closely resembles the original without any material alteration.

2. Documents shall be in a format that provides for browser accessibility and no material alteration to content or appearance. Documents shall be formatted in either:

   a. PDF (Portable Document Format) version 2.x or higher; or

   b. XML (Extensible Markup Language), after the supreme court adopts standards for its use.

3. Hyperlinks, bookmarks and other similar navigational functions shall only refer to other parts in the same document.

4. Graphics, multimedia and other non-text documents may be permitted as follows:

   a. Documents in imaged or graphic formats (for example, pictures or maps) shall be in a non-proprietary file format (for example, TIFF, GIF, or JPEG) and shall comply with ACJA '1-504.

   b. Other multimedia files (for example, video or audio files) shall adhere to established industry standards and shall be in a non-proprietary format (for example, MPEG, AVI, and WAV). Each court implementing electronic filing has the discretion to accept or reject any other video or graphic format.

5. E-mail communications may be used for receipt, confirmation, and notification correspondence, and, if permitted by a court=s electronic document filing procedures, as a method of transporting documents.

6. An electronic filing system may provide fill-in forms for routine matters such as traffic citations or small claims filings. The forms-based electronic filing system shall be capable of reproducing or printing the form with the data supplied by the filer, however, courts are not required to preserve

the form's text and data together in PDF. The forms-based electronic filing system shall comply with all other requirements of this section.

E. Authentication.

1. Authentication of document source. Any court implementing electronic filing shall establish a procedure to verify and authenticate the source of electronically filed documents. Acceptable procedures include:

    a. Electronic or digital signature and certificate;

    b. User ID and password;

    c. Credit card authentication; or

    d. Other equivalent procedure.

2. Authentication of documents. To prevent alteration during transmission, any court implementing electronic filing shall establish a procedure for assuring that documents filed electronically have not been altered during transmission. Acceptable procedures include:

    a. A checksum or hashing algorithm;

    b. Digital time-stamps;

    c. Digital certificates using PKI which provides for encapsulation of the message in such a way that altering it invalidates the associated certificate, or

    d. Other equivalent procedure.

3. Maintenance of electronic documents. Any court implementing electronic filing shall employ security procedures that prevent unauthorized modification or deletion of the electronically filed document. These procedures shall include all of the following:

    a. Establishing written procedures to ensure the integrity of electronic documents, so that any copies produced may be regarded as true and correct copies of the original document;

    b. Performing virus checking to ensure documents are free from viruses;

    c. Employing procedures that insure the availability of at least one other copy of the electronically filed document at all times;

d. Performing system backups at least daily;

e. Using recording media for storing electronic records that comply with ANSI/AIIM standards; and

f. Using non-reusable media for archiving court records electronically.

4. Filing of confidential and sealed documents. Courts shall not accept electronically filed confidential and sealed documents.

F. Communications. The electronic filing system implemented by any court shall:

1. Provide for electronic filing via the Internet or other publicly accessible mechanism;

2. Use industry-standard, non-proprietary protocols such as FTP; and

3. Provide for appropriate public access, with preference given to standard browser technology.

G. Processing.

1. Each electronic filing system shall generate an acknowledgment receipt for electronically filed documents.

2. Each electronic filing system shall be implemented with an automated interface to that court=s case management and electronic document management systems that will:

a. Provide and verify case management data;

b. Automatically docket documents; and

c. Automatically index documents as required for locating the document and facilitating integration with the case and document management systems. Indexing elements may include:

(1) Case number;
(2) Document type;
(3) Filing party information; or
(4) Date filed.

3. The electronic filing system shall provide appropriate public access. Every court implementing

electronic filing shall ensure that its electronic filing system complies with ACJA '1-504 (C).

4. Prior to accepting electronic filings, each court implementing an electronic filing system shall develop an electronic filing plan that includes at least the following:

   a. Hardware and software acquisition, installation, and implementation;

   b. Testing, training, staffing and support;

   c. Integration with the document and case management systems; and

   d. Security and document availability.

5. Each court implementing an electronic filing system shall electronically publish detailed procedures for use of its electronic filing system, that include at least the following elements:

   a. Filing procedures, including whether a party who electronically files a document is relieved from any obligation to file additional copies with the court, as may be required by local rule, and hours of availability;

   b. Practices for acknowledgment of receipt and exception processing; and

   c. Procedures for addressing transmission difficulties and obtaining assistance.

H. Periodic Review. These requirements are designed to be flexible to allow for technical innovations and shall be reviewed annually by the Commission on Technology and updated to adapt to technological changes.

Adopted by Administrative Order 2001-116 effective December 7, 2001.